UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
JACKSONVILLE DIVISION

In re Brinker Data Incident Litigation

Case No. 3:18-cv-686-J-32MCR

ORDER

Customers of Chili's Grill & Bar learned their payment card information had been compromised by hackers. This class action against Chili's parent, Brinker, Inc., seeks redress for that incident. It is before the Court on Defendant Brinker, Inc.'s Rule 12(b)(6) Motion to Dismiss. (Doc. 48). Plaintiffs responded, (Doc. 53), Brinker replied, (Doc. 54), and Plaintiffs filed a sur-reply, (Doc. 57). On June 25, 2019, the Court held a hearing on the motion, the record of which is incorporated herein. (Doc. 63). Following the hearing, the parties filed supplemental briefing on choice of law. (Doc. 68).

I. BACKGROUND

A. Alleged Facts

According to the Second Amended Consolidated Complaint ("the complaint"), beginning in March 2018, hackers accessed Brinker's data network and installed malware on point-of-sale ("POS") systems [1] at many Chili's restaurants, which Brinker owns, develops, operates, and franchises. (complaint, Doc. 39 ¶¶ 25, 101). Brinker publicly announced the breach on May 12, 2018, stating:

> On May 11th, 2018, we learned that payment card information of some of our Guests who visited certain Chili's® Grill & Bar corporate-owned restaurants have been compromised in a data incident. Currently, we believe the data incident was limited to between March – April 2018; however, we continue to assess the scope of the incident.
>
> Upon learning of this incident, we immediately activated our response plan. We are working with third-party forensic experts to conduct a thorough investigation to determine the details of what happened. Law enforcement has been notified of this incident and we will continue to fully cooperate.

---

[1] According to the complaint:

> A POS system is an on-site device, much like an electronic cash register, which manages transactions from consumer purchases, both by cash and card. When a payment card is used at a POS terminal, "data contained in the card's magnetic stripe is read and then passed through a variety of systems and networks before reaching the retailer's payment processor." The payment processor then passes the payment information on to the financial institution that issued the card and takes the other steps needed to complete the transaction.

(Doc. 39 ¶ 75) (citations omitted).

> While the investigation is still ongoing, we believe that malware was used to gather payment card information, including credit or debit card numbers and cardholder names, from our payment-related systems for in-restaurant purchases at certain Chili's restaurants.
>
> We deeply value our relationships with our Guests and our priority remains doing what is right for them. We are committed to sharing additional information on this ongoing investigation. More details can be found at: http://brinker.mediaroom.com/ChilisDataIncident.

(Id. ¶ 102).

Brinker acknowledges that it relies on information systems, and "Chili's has long touted its technological innovation . . . ." (Id. ¶¶ 60, 62). Chili's daily payment card transactions are in the "tens of thousands . . . ." (Id. ¶ 72). When Brinker processes payment card transactions, it collects "the cardholder name, the account number, expiration date, card verification value ("CVV"), and PIN data for debit cards. Brinker stores th[is] Customer Data in its POS system and transmits this information to a third party for processing and completion of the payment." (Id. ¶ 64).

The number of data breaches involving the theft of retail payment card information has been rising over the past several years, and "[m]ost of the massive data breaches occurring within the last several years involved malware placed on POS systems used by merchants." (Id. ¶¶ 74–75). These breaches include other national restaurant chains, such as P.F. Chang's, Arby's, Chipotle, and Wendy's. (Id. ¶ 103). "Given the numerous reports indicating the

susceptibility of POS systems and consequences of a breach, Brinker was well-aware, or should have been aware, of the need to safeguard its POS systems." (Id. ¶ 80). Plaintiffs allege that despite this knowledge, Brinker failed to comply with industry standards for information security, including the Payment Card Industry Data Security Standard ("PCI DSS"). (Id. ¶¶ 81–90). And, "Brinker failed to implement adequate data security measures to protect its POS networks from the potential danger of a data breach and failed to implement and maintain reasonable security procedures and practices . . . ." (Id. ¶ 106). Specifically, "Brinker operated POS systems with outdated operating systems and software; failed to enable point-to-point and end-to-end encryption; and, failed to take other measures necessary to protect its data network." (Id. ¶ 98).

During the data breach, each of the named plaintiffs paid for food and services at a Chili's restaurant with their credit or debit card. Marlene Green-Cooper dined at a Chili's in Florida in April 2018, and "[w]ithin days thereafter" noticed three unauthorized charges on the credit card she had used at Chili's. (Id. ¶¶ 28(1)–29(1)). Green-Cooper was issued a new credit card and during the time she waited for a new card she lost the ability to accrue cash back rewards. (Id. ¶¶ 28(1)–28(2)).[2] Green-Cooper continues to monitor her account daily for unauthorized charges. (Id. ¶ 29(1)).

[2] Plaintiffs have two paragraphs numbered "28" and two numbered "29." This Order denotes them as 28(1) and 28(2).

In April 2018, Shenika Thomas used her debit card at a Chili's in Texas. (Id. ¶ 29(2)). In early May 2018, Thomas incurred three fraudulent charges totaling more than $100 on her debit card. (Id. ¶ 30). Thomas was issued a new debit card, and she, too, continues to monitor her account to prevent further misuse. (Id.).

Between March and April 2018, Michael Franklin used his payment cards at various Chili's locations in California. (Id. ¶¶ 34–44). After using a payment card three times in two months at Chili's, Franklin experienced fraudulent charges on his account, spent time speaking with his bank, and lost the chance to accrue rewards points while awaiting a replacement card. (Id. ¶¶ 44–46).

In April 2018, Eric Steinmetz used his debit card at a Chili's in Nevada. After learning of the breach, Steinmetz "procured his consumer disclosures from all three credit reporting agencies," "incurred transportation costs of gasoline in driving to Wells Fargo to cancel his debit card and obtain a temporary card[,]" and "lost time dealing with issues related to the [data breach] . . . ." (Id. ¶¶ 47–49).

Plaintiffs allege that they would not have dined at Chili's had they known "it lacked adequate computer systems and data security practices to safeguard" customers' information. (Id. ¶ 50). Plaintiffs further allege that the value of their customer data has diminished, they lost time, have been inconvenienced, and "have concerns for the loss of their privacy." (Id. ¶¶ 53–54). Additionally,

Plaintiffs face a "substantially increased risk of fraud, identity theft, and misuse resulting from" the data breach. (Id. ¶ 55).

B. Procedural Posture

On October 30, 2018, the Court consolidated several related cases with this one, and directed Plaintiffs to file an amended consolidated complaint. (Doc. 31). Plaintiffs filed the operative Second Amended Consolidated Class Action Complaint, (Doc. 39), which alleges fourteen causes of action.[3] The eight named plaintiffs seek certification of a Nationwide Class, which is defined as: "All persons residing in the United States who made a credit or debit card purchase at any affected Chili's location during the period of the Data Breach. . . ." (Id. ¶ 129). In the alternative, Plaintiffs propose separate Statewide classes, which are defined as: "All persons residing in [California, Florida, Virginia, Nevada, or Texas] who made a credit or debit card purchase at any affected Chili's location during the period of the Data Breach (the 'Statewide Classes')." (Id. ¶ 130).

The complaint charges six common law claims on behalf of the Nationwide Class, or in the alternative on behalf of each Statewide Class: breach of implied contract (Count I); negligence (Count II); negligence per se (Count III); unjust enrichment (Count IV); declaratory judgment (Count V); and

[3] Plaintiffs mistakenly have two Counts numbered "XII." This order refers to the second Count XII as XII(b).

breach of confidence (Count XIII). Each Statewide Class also alleges state statutory violations: Florida Deceptive and Unfair Trade Practices Act ("FDUTPA") (Count VI); Texas Deceptive Trade Practices-Consumer Protection Act ("Texas DTPA") (Count VII); Virginia Customer Data Breach Notification Act ("Virginia Notification Act") (Count VIII); Virginia Consumer Protection Act ("VCPA") (Count IX); California's Unfair Competition Law ("UCL") – Unlawful Business Practices (Count X); California's UCL – Unfair Business Practices (Count XI); California's UCL – Fraudulent/Deceptive Business Practices (Count XII); and Nevada's Consumer Fraud Act ("CFA") (Count XII (b)).

Brinker moved to dismiss every count under Rule 12(b)(6) for failing to state a claim, and to dismiss the case under Rule 12(b)(1), arguing that the named plaintiffs lack standing. (Doc. 48). The Court ruled on Brinker's Rule 12(b)(1) motion to dismiss in a separate Order, (Doc. 65), finding that Plaintiffs, Christopher Lang and Peter Alamillo failed to allege an injury in fact, but that all other named plaintiffs had standing. In that Order, the Court deferred ruling on the Rule 12(b)(6) portion of Brinker's motion. The Court also requested that the parties file a joint notice indicating how they would like to proceed regarding the choice of law concerns the Court raised at the hearing. (Doc. 65). The parties filed their joint notice but could not agree on how to proceed. (Doc. 68). Plaintiffs subsequently dismissed two named plaintiffs: Fred

Sanders and Daniel Summers. (Docs. 71, 72, 73).[4] After the parties filed several discovery motions, (Docs. 77, 79, 80, 82, 84), the Court stayed all depositions and new discovery requests pending the Court's ruling on the motion to dismiss. (Doc. 85). Of those requests, only Brinker's Motion for Protective Order remains. (Doc. 84).

II. CHOICE OF LAW

The parties briefing on the motion to dismiss did not address choice of law. Many of the common law claims were analyzed under Florida law, but the parties also relied on data breach cases that applied different states' laws. Because the Court was unclear on which states' laws applied to the common law claims, it requested that the parties determine whether they wanted to brief choice of law now, or have the Court defer ruling on the Rule 12(b)(6) portion of the motion to dismiss until the class certification stage (when the Court would receive choice of law briefing). (Doc. 65). In response to the Court's Order, (Doc. 65), the parties filed a joint notice on how the case should proceed regarding choice of law for the motion to dismiss. (Doc. 68).

Unfortunately, the parties do not agree on how the Court should handle choice of law. Plaintiffs want the Court to defer ruling on the Rule 12(b)(6) motion to dismiss and brief choice of law just before the class certification

[4] As Sanders was the only Virginia named plaintiff, the claims on behalf of the Virginia Statewide Class (Counts VIII and IX) are due to be dismissed.

motion. They claim they need additional discovery to inform the choice of law analysis. (Id. at 6–7). Brinker asserts that no additional discovery is needed and that the parties can brief, and the Court can decide, the choice of law issues now. (Id. at 2). Despite relying primarily on Florida law in its Motion to Dismiss, Brinker now argues that Texas law governs each of Plaintiffs' common law claims.

The parties originally relied on Florida law, and now they cannot decide what law applies to the common law claims. Instead of further briefing on choice of law for the motion to dismiss, the Court will analyze the common law claims primarily under Florida law (as was briefed by the parties) and will address the other states' laws if dispositive differences arise. See Wilding v. DNC Servs. Corp., 941 F.3d 1116, 1127 (11th Cir. 2019); Sun Life Assurance Co. of Canada v. Imperial Premium Fin., LLC, 904 F.3d 1197, 1208 (11th Cir. 2018) ("Under our precedents, a party waives its opportunity to rely on non-forum law where it fails to timely provide—typically in its complaint or the first motion or response when choice-of-law matters—the sources of non-forum law on which it seeks to rely.").[5]

[5] The decision to apply Florida law to the common law claims does not violate due process. Cf. Phillips Petroleum Co. v. Shutts, 472 U.S. 797, 821 (1985) (finding that applying Kansas law to all class action claims where 97% of the plaintiffs had no connection with Kansas violated the constitutional limits imposed on choice of law). At the motion to dismiss stage, the Court considers the allegations of the Named Plaintiffs. Parm v. Nat'l Bank of Cal.,

III. SUFFICIENCY OF THE COMPLAINT

Defendants move to dismiss each count in the complaint as failing to state a claim upon which relief can be granted. (Doc. 48). The Court will analyze each claim in turn.

A. Breach of Implied Contract (Count I)

Under Florida law, breach of an implied contract is analyzed the same as breach of an express contract, Resnick v. AvMed, Inc., 693 F.3d 1317, 1325 (11th Cir. 2012), requiring the plaintiff to allege: (1) existence of a contract; (2) a material breach of the contract by the defendant; and (3) damages resulting from the defendant's breach of the contract. Mink v. Smith & Nephew, Inc., 860 F.3d 1319, 1332 (11th Cir. 2017).[6]

N.A., 242 F. Supp. 3d 1321, 1342 (N.D. Ga. 2017) ("When considering a motion to dismiss filed in a putative class action before certification of a class, the Court considers only Plaintiff's individual allegations . . . , not the generalized allegations of the putative class members."). This means that only four states' laws could apply: Florida, California, Nevada, and Texas. Although Named Plaintiffs cannot consent to the law to be applied to the absent class members, Shutts, 427 U.S. at 820, courts commonly rely upon the law briefed in deciding a motion to dismiss without conducting a fact-intensive choice of law analysis. See, e.g., McKenzie v. Allconnect, Inc., 369 F. Supp. 3d 810, 817 (E.D. Ky. 2019); Davidson v. Apple, Inc., No. 16-CV-4942-LHK, 2017 WL 3149305, at *3 (N.D. Cal. July 25, 2017). Thus, at the class certification and summary judgment stage, the Court will need to conduct a detailed choice of law analysis. But for now, the Court may proceed under Florida law, supplemented as appropriate with several cases from other jurisdictions.

[6] Nevada law has the same elements for breach of contract. See S. Fork Livestock P'ship v. United States, 183 F. Supp. 3d 1111, 1118 (D. Nev. 2016). California and Texas law have four elements: "To plead breach of an implied contract, a plaintiff must allege: '(1) the contract, (2) plaintiff's performance or

1. Plaintiffs have pled the existence of an implied contract.

To establish the existence of a contract under Florida law, the plaintiff must show offer, acceptance, consideration, and specificity in terms of the contract. Mink, 860 F.3d at 1332. Implied contracts are inferred in whole or in part from the parties' conduct. Cableview Commc'ns of Jacksonville, Inc. v. Time Warner Cable Se., LLC, No. 3:13-CV-306-J-JRK, 2017 WL 5240208, at *16 (M.D. Fla. Jan. 4, 2017), aff'd, 901 F.3d 1294 (11th Cir. 2018). When considering whether an implied contract exists, a court should give "the effect which the parties, as fair and reasonable men, presumably would have agreed upon if, having in mind the possibility of the situation which has arisen, they had contracted expressly thereto." Bromer v. Fla. Power & Light Co., 45 So. 2d 658, 660 (Fla. 1950). Because the parties' conduct is central to determining whether an implied contract was formed, this determination is typically left for the fact finder. See Commerce P'ship 8098 Ltd. P'ship v. Equity Contracting Co., 695 So. 2d 383, 385 (Fla. 4th DCA 1997), as modified on clarification (June

---

excuse for nonperformance, (3) defendant's breach, and (4) the resulting damages to plaintiff.'" Castillo v. Seagate Tech., LLC, No. 16-CV-01958-RS, 2016 WL 9280242, at *8 (N.D. Cal. Sept. 14, 2016) (quoting Reichert v. Gen. Ins. Co. of Am., 68 Cal. 2d 822, 830 (1968)); Thymes v. Gillman Cos., No. CV H-17-2834, 2018 WL 1281852, at *2 (S.D. Tex. Mar. 9, 2018) (same). This additional element makes no difference here because the plaintiffs have alleged that they completed their performance—paid for their food and drink at Chili's.

4, 1997) ("[A] fact finder must examine and interpret the parties' conduct to give definition to their unspoken agreement.").

The majority of federal courts have held that the existence of an implied contract to safeguard customers' data could reasonably be found to exist between a merchant and customer when a customer uses a payment card to purchase goods and services. See Resnick, 693 F.3d at 1327–28 (applying Florida law, the court denied a motion to dismiss a breach of implied contract claim where customers' personal healthcare information was stolen from the defendant, and causation and damages were sufficiently pled); Torres v. Wendy's Int'l, LLC (Torres II), No. 6:16-cv-210-Orl-40DCI, 2017 WL 8780453, at *3 (M.D. Fla. Mar. 21, 2017). In Torres II, a similar data breach action against Wendy's, the court found that a reasonable jury could infer that the parties' conduct created an implied contract that Wendy's, by inviting customers to pay with payment card, would safeguard its customers' data. 2017 WL 8780453, at *3; see also Castillo, 2016 WL 9280242, at *9 (applying California law) ("Plaintiffs' claim is a far more realistic reflection of the mutual agreement that occurs in most data-sharing transactions: When a person hands over sensitive information, in addition to receiving a job, good, or service, they presumably expect to receive an implicit assurance that the information will be protected.").

Other courts have found that a transaction for services does not create an implied contract to protect data beyond the privacy requirements already imposed by federal law. Brush v. Miami Beach Healthcare Grp. Ltd., 238 F. Supp. 3d 1359, 1369 (S.D. Fla. 2017) (applying Florida law); see also, e.g., Lovell v. P.F. Chang's China Bistro, Inc., No. C14-1152RSL, 2015 WL 4940371, at *3 (W.D. Wash. Mar. 27, 2015) ("Plaintiff alleges no facts suggesting that he requested or that defendant made additional promises regarding loss prevention, and neither the circumstances nor common understanding give rise to an inference that the parties mutually intended to bind defendant to specific cybersecurity obligations.").[7]

Here, the Court must look to the parties' conduct to determine if an implied contract exists. Similar to the plaintiffs in Torres II, Plaintiffs allege they were "solicited and invited" by Brinker to "eat at its restaurants and make purchases using their credit or debit cards." (Doc. 39 ¶ 143). Also like the plaintiffs in Torres II, Plaintiffs allege they entered into implied contracts with

[7] Brinker also cites additional cases, such as Irwin v. Jimmy John's Franchise, LLC, 175 F. Supp. 3d 1064, 1070–71 (C.D. Ill. 2016) to argue that "numerous cases around the country . . . have repeatedly rejected Plaintiffs' precise theory of recovery[—breach of implied contract]." However, in discussing the breach of implied contract claim, Irwin held: "Irwin has alleged the existence of an implied contract obligating Jimmy John's to take reasonable measures to protect Irwin's information and to timely notify her of a security breach." Brinker's cherry-picked quote from Irwin was in that court's discussion of unjust enrichment.

Brinker. (Doc. 39 ¶ 144). Plaintiffs believe the contract, embedded in the invitation to pay with payment cards, contained an agreement that Brinker would utilize Plaintiffs' confidential information for the agreed payment and nothing else, thereby creating an obligation that Brinker "use reasonable measures to safeguard and protect Customer data." (Id. ¶ 145). A fact finder could reasonably construe this conduct to create an implied contract.

Cases reaching the opposite conclusion are distinguishable or unpersuasive. In Brush, there is no evidence that the defendant advertised its services, whereas cases finding an implied contract have found significant the invitation to pay with a card. See Brush, 238 F. Supp. 3d at 1368–69. Further, Brush focuses on the privacy requirements already imposed by federal law—i.e. HIPAA—and it fails to distinguish Resnick or discuss why it is not controlling. Id. Thus, Plaintiffs have alleged an implied contract under Florida law.

2. Plaintiffs have pled that Brinker's material breach caused Plaintiffs' damages.

For a breach to be material, a party's nonperformance must "go to the essence of the contract." Britt Green Trucking, Inc. v. FedEx Nat., LTL, Inc., No. 8:09-CV-445-T-33TBM, 2014 WL 3417569, at *6 (M.D. Fla. July 14, 2014) (quoting Covelli Family, LP v. ABG5, L.L.C., 977 So. 2d 749, 752 (Fla. 4th DCA 2008)). Assuming the parties had an implied contract requiring Brinker to safeguard Plaintiffs' information—an essential obligation of the alleged implied

contract—the theft of that information is sufficient to demonstrate a breach at this stage of the proceedings. (Doc. 39 ¶ 2, n.1).

Plaintiffs must also show that the breach of the implied contract caused their damages. Resnick, 693 F.3d at 1325. This requires "allegations of a nexus between [the data breach and the damages] beyond allegations of time and sequence." Id. at 1326. There must be "a logical connection between the two incidents." Id. at 1327. In Resnick, two laptops containing the defendant's customers' sensitive information were stolen from the defendant's office. Id. at 1322. Ten months after the theft, two of the defendant's customers (the plaintiffs) had their sensitive information used to open bank accounts and make unauthorized purchases. Id. The Eleventh Circuit held that the breach of implied contract claim could survive, despite a ten-month gap between the breach and the data being compromised, because the information stolen was the same information needed to open bank accounts in the customers' names, satisfying the logical connection. Id. at 1327.

Plaintiffs have pled enough facts to show causation. Several named Plaintiffs experienced fraudulent charges on their account between a few days to four weeks after using a payment card at a Chili's. (Doc. 39 ¶¶ 29(1), 31–32, 34–35, 43–44). Additionally, like the information used to open accounts in Resnick, the fraudulent charges here required the same information that was

stolen from Brinker (payment card numbers, expiration dates, and CVV or PINs), satisfying the logical connection.

3. Plaintiffs have sufficiently pled damages.

Under Florida law, breach of contract damages are typically limited to compensatory damages, see MCI Worldcom Network Servs., Inc. v. Mastec, Inc., 995 So. 2d 221, 223 (Fla. 2008), that "naturally flow from the breach," Kakawi Yachting, Inc. v. Marlow Marine Sales, Inc., No. 8:13-CV-1408-T-TBM, 2014 WL 12650104, at *8 (M.D. Fla. Apr. 11, 2014). Damages in a breach of contract action cannot be too speculative. Casey v. Bank of Am., N.A., No. 13-60983-CIV, 2014 WL 12580515, at *3 (S.D. Fla. Mar. 12, 2014) (holding the plaintiff failed to satisfy the damages element of a breach of contract claim because the plaintiff alleged only possible negative impacts on his credit report and history and no "tangible pecuniary loss").

In data breach cases, courts are divided on whether plaintiffs must plead that their fraudulent charges were unreimbursed. Compare Resnick, 693 F.3d at 1324 (holding plaintiffs need only allege losses, not unreimbursed losses, for a cognizable injury in a Florida breach of implied contract claim), with In re SuperValu, Inc., Customer Data Sec. Breach Litig., No. 14-MD-2586 ADM/TNL, 2018 WL 1189327, at *12 (D. Minn. Mar. 7, 2018) (holding allegations of fraudulent charges alone are insufficient for damages in breach of implied contract claim under Illinois law), aff'd, No. 18-1648, 2019 WL 2306267 (8th Cir.

May 31, 2019). Most courts find some type of economic loss sufficient, Resnick, 693 F.3d at 1324, but that time spent monitoring accounts is too speculative to constitute damages, Pisciotta v. Old Nat. Bancorp, 499 F.3d 629, 635 (7th Cir. 2007) (applying Indiana law the court held that without allegations of increased risk of future identity theft, allegations of credit monitoring costs are too speculative). Here, under Florida law, the fraudulent charges are sufficient for damages for breach of implied contract.[8] See Resnick, 693 F.3d at 1324. Thus, Brinker's motion to dismiss Plaintiffs' breach of implied contract claim is denied.

B. Negligence (Count II)

Brinker moves to dismiss Plaintiffs' negligence claim by arguing that it had no duty (and therefore no breach) and that Plaintiffs have no damages. To maintain a claim for negligence under Florida law, Plaintiffs "must allege four elements: a duty, breach of that duty, causation, and damages." Virgilio v.

[8] The Eighth Circuit has required plaintiffs in data breach cases to plead that their fraudulent charges were not reimbursed to sufficiently allege damages. In re SuperValu *II*, 925 F.3d at 965 (finding that it was unreasonable, based on federal law and "common sense," to infer in plaintiffs' favor that their fraudulent charges went unreimbursed). Although this is an interesting argument, it is inconsistent with Eleventh Circuit precedent. Resnick, 693 F.3d at 1324 (finding as specious the argument that under Florida law plaintiffs do not have cognizable damages because they did not allege their fraudulent charges went unreimbursed).

Ryland Grp., Inc., 680 F.3d 1329, 1339 (11th Cir. 2012) (citing Curd v. Mosaic Fertilizer, L.L.C., 39 So. 3d 1216, 1227 (Fla. 2010)).

1. Plaintiffs have alleged a duty.

Whether a duty exists under Florida negligence law is a question for the court. Id. (citing Williams v. Davis, 974 So. 2d 1052, 1057 n. 2 (Fla. 2007)). When a plaintiff seeks to impose a duty based on the particular facts alleged (as opposed to one imposed by legislative or administrative enactments or judicial precedent), the court must evaluate and apply "the concept of foreseeability of the harm to the circumstances alleged . . . ." United States v. Stevens, 994 So. 2d 1062, 1066–67 (Fla. 2008). "Under Florida law, 'where a defendant's conduct creates a foreseeable zone of risk, the law generally will recognize a duty placed upon defendant either to lessen the risk or see that sufficient precautions are taken to protect others from the harm that the risk poses.'" Ombres v. City of Palm Beach Gardens, 788 F. App'x 665, 667 (11th Cir. 2019) (citing Kaisner v. Kolb, 543 So. 2d 732, 735 (Fla. 1989)).

In Stevens, the Florida Supreme Court reiterated that the foreseeable zone of risk test is appropriate to determine whether a duty exists. Id. In that case, the plaintiff alleged that a medical laboratory was negligent in securing biohazardous materials (including anthrax) that were later used by terrorists to kill the plaintiff's husband. Id. at 1064. In determining that the laboratory owed a duty, despite the intervention of third-party criminals, the Florida

Supreme Court relied on § 302B of the Restatement (Second) of Torts, which states: "An act or an omission may be negligent if the actor realizes or should realize that it involves an unreasonable risk of harm to another through the conduct of . . . a third person which is intended to cause harm, even though such conduct is criminal." Id. at 1067 (quoting Restatement (Second) of Torts §§ 302-302B (1965)). Further, comment "e" to section 302B provides that "an actor 'is required to anticipate and guard against the intentional, or even criminal, misconduct of others' . . . 'where the actor's own affirmative act has created or exposed the other to a recognizable high degree of risk of harm through such misconduct, which a reasonable man would take into account . . . .'" Id. (quoting Restatement (Second) of Torts § 302B cmt. e)).

The acts here are "acts of commission, which historically generate a broader umbrella of tort liability than acts of omission . . . ." Stevens, 994 So. 2d at 1068 (quoting Stevens v. United States, No. 9:03-cv-81110-DTKH, slip op. at 9 (Apr. 15, 2005), ECF No. 47). Although Brinker attempts to characterize the acts as an omission—failure to properly secure data—the commission was the alleged negligent collection and storage of personal information and payment card data. See id. at 1069 n.4 (explaining the difference between affirmative acts—misfeasance—and omissions to act—nonfeasance).

Plaintiffs have alleged that Brinker owed a duty to use reasonable care in protecting customers' personal and payment card information. Plaintiffs

allege that Brinker failed "to properly protect the Customer Data, despite being aware of recent data breaches impacting other national restaurant chains . . . ." (Doc. 39 ¶ 103). Further, Plaintiffs allege that Brinker was aware of other breaches involving malware installed on point of sale systems, (id. ¶ 80), and it was aware that its point of sale systems could be targeted, (id. ¶ 99), yet it nonetheless failed to implement "reasonable and sufficient protective measures to prevent the Data Breach[,]" (id. ¶ 82). These facts sufficiently allege a duty. See Torres II, 2017 WL 8780453, at *4 (finding that allegations that "Wendy's had ample reasons to anticipate the hack, but failed to take action to prevent it" was sufficient to allege a foreseeable zone of risk).

Brinker's argument that Florida law does not protect against the wrongdoing of third parties, is misplaced. (Doc. 48 at 32 (citing Knight v. Merhige, 133 So. 3d 1140, 1145 (Fla. 4th DCA 2014))). In Knight, the Fourth DCA stated that no duty was imposed upon the parents for their adult son's murders because, despite being foreseeable, the parents exerted no control over their adult son and had no special relationship with the plaintiffs. 133 So. 3d at 1145–46. Here, Brinker, by collecting personal information and payment card data, had control over the information and had a duty to use reasonable care in protecting that data from theft.

2. Plaintiffs' damages.

Brinker fails to address a single Florida case in its section addressing damages for negligence. Both sides equate damages with Article III's injury in fact requirement, which is not always correct. They may overlap but are not synonymous.

Florida defines damages in negligence cases as "some actual harm." Am. Optical Corp. v. Spiewak, 73 So. 3d 120, 127 (Fla. 2011) (quoting Williams v. Davis, 974 So. 2d 1052, 1056 (Fla. 2007)). Some of the named Plaintiffs have alleged that they incurred fraudulent charges on their payment cards, which is sufficient for damages. Resnick, 693 F.3d at 1324 ("[M]onetary loss is cognizable under Florida law for damages in contract, quasi-contract, negligence, and breach of fiduciary duty."). Brinker argues that these damages are insufficient because Plaintiffs did not allege the charges were unreimbursed. However, Plaintiffs did not allege that the charges were reimbursed—only that they incurred fraudulent charges. These allegations are sufficient to withstand a motion to dismiss.[9] See Resnick, 693 F.3d at 1324 ("AvMed contends that Plaintiffs' injuries are not cognizable under Florida law because the Complaint alleges only 'losses,' not 'unreimbursed losses.' This is a specious argument.").

[9] See supra note 8.

Whether, and in what amount, Plaintiffs can prove damages at summary judgment or trial remains to be seen.

Thus, Plaintiffs have sufficiently alleged negligence under Florida law.[10]

C. Negligence Per Se (Count III)

Plaintiffs assert a claim for negligence per se, based on Brinker's violation of § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act"). Brinker argues that Plaintiffs have failed to allege a cause of action for negligence per se.

> A negligence per se claim would be appropriate under Florida law when there is a violation of a "statute which establishes a duty to

[10] However, the economic loss rule in California and possibly Nevada and Texas may bar the negligence claims under those states' laws. See Gordon v. Chipotle Mexican Grill, Inc., 344 F. Supp. 3d 1231, 1246 (D. Colo. 2018) ("The Court therefore concludes that California's economic loss doctrine does bar Plaintiffs' negligence claim."); In re Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1172 (D. Minn. 2014) ("Plaintiffs' California negligence claims are dismissed on the basis of the economic loss rule."); Lone Star Nat. Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421 (5th Cir. 2013) (acknowledging, in a data breach case, that the parties agreed the economic loss rule under Texas law would bar plaintiffs negligence claim); Terracon Consultants W., Inc. v. Mandalay Resort Grp., 206 P.3d 81, 86 (Nev. 2009) ("[T]his court has concluded that the doctrine bars unintentional tort actions when the plaintiff seeks to recover "purely economic losses." (quotation and citations omitted)). Additionally, in In re Sony, the court, applying California law, stated "without specific factual statements that Plaintiffs' Personal Information has been misused, in the form of an open bank account, or un-reimbursed charges, the mere 'danger of future harm, unaccompanied by present damage, will not support a negligence action.'" In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 963 (S.D. Cal. 2012). However, that case did not involve theft of payment card information and did not have allegations of fraudulent charges, so the court's statement may not control the situation here.

> take precautions to protect a particular class of persons from a particular injury or type of injury." Additionally, a plaintiff pursuing a negligence per se claim must also establish that she "is of the class the statute was intended to protect, that [s]he suffered injury of the type the statute was designed to prevent, and that the violation of the statute was the proximate cause of h[er] injury."

Liese v. Indian River Cty. Hosp. Dist., 701 F.3d 334, 353 (11th Cir. 2012) (quoting deJesus v. Seaboard Coast Line R. Co., 281 So. 2d 198, 200 (Fla. 1973)). Courts have used this standard to hold that a negligence per se claim cannot rest on a federal statute that does not provide a private right of action. Weinberg v. Advanced Data Processing, Inc., 147 F. Supp. 3d 1359, 1365 (S.D. Fla. 2015) (compiling cases). "When a statute is silent as to whether it allows for a private cause of action, such a claim can only survive when the statute evidences legislative intent to create a private cause of action." Zarrella v. Pac. Life Ins. Co., 755 F. Supp. 2d 1218, 1228 (S.D. Fla. 2010) (citing Murthy v. N. Sinha Corp., 644 So.2d 983, 985 (Fla. 1994)). "There is no private cause of action implied under the Federal Trade Commission Act." Lingo v. City of Albany Dep't of Cmty. & Econ. Dev., 195 F. App'x 891, 894 (11th Cir. 2006); see also In re SuperValu, Inc., 925 F.3d at 963–64 (declining to impose a duty based on the FTC Act because "Congress empowered the Commission—and the Commission alone—to enforce the FTCA. Implying a cause of action would be inconsistent with Congress's anticipated enforcement scheme."). Thus, violation of the FTC Act cannot be the basis for a negligence per se claim.

Plaintiffs assert that even if the Court dismisses their negligence per se claim, it should allow Plaintiffs to maintain their negligence action under the same duty—the FTC Act. (Doc. 53 at 30). Dismissal of Count III would not preclude Plaintiffs from arguing that a violation of the FTC Act is evidence of negligence. "[T]he Florida Supreme Court has noted that when a cause of action for negligence per se fails because the statute at issue does not expressly provide for one, a plaintiff still has a 'right to bring a common law negligence claim based upon the same allegations.'" St. Cyr v. Flying J Inc., No. 3:06-cv-13-J-33TEM, 2006 WL 2175662, at *6 (M.D. Fla. July 31, 2006) (quoting Villazon v. Prudential Health Care Plan, Inc., 843 So. 2d 842, 852 (Fla. 2003)). However, "any regulation that purports to establish a duty of reasonable care must be specific. One that sets out only a general or abstract standard of care cannot establish negligence." Murray v. Briggs, 569 So. 2d 476, 481 (Fla. 5th DCA 1990) (citations omitted).

Plaintiffs have failed to allege a specific duty imposed by the FTC Act. See id.; Estate of Johnson ex rel. Johnson v. Badger Acquisition Of Tampa LLC, 983 So. 2d 1175, 1182 (Fla. 2d DCA 2008) ("[T]he violation of a statute may be evidence of negligence, but such evidence only becomes relevant to a breach of a standard of care after the law has imposed a duty of care."). Plaintiffs allege that Brinker failed to comply with FTC "guidelines" and "recommendations," not any specific duty of reasonable care mandated by the FTC Act. Therefore,

Plaintiffs should not be able to premise its breach of a duty solely on Brinker's alleged violation of the FTC Act. However, Plaintiffs should be able to use the FTC Act as evidence that the data breach was within the foreseeable zone of risk.[11] Count III is due to be dismissed.

D. Unjust Enrichment (Count IV)

Plaintiffs have failed to plead an unjust enrichment claim. Under Florida law, a claim for unjust enrichment requires that: (1) the plaintiff has conferred a benefit on the defendant; (2) the defendant has knowledge of the benefit; (3) the defendant has accepted or retained the benefit conferred; and (4) the circumstances are such that it would be inequitable for the defendant to retain the benefit without paying fair value for it. Resnick, 693 F.3d at 1328 (quoting Della Ratta v. Della Ratta, 927 So. 2d 1055, 1059 (Fla. 4th DCA 2006)).

---

[11] This result appears to be consistent with California, Nevada, and Texas law. Gordon v. Chipotle Mexican Grill, Inc., No. 17-CV-1415-CMA-MLC, 2018 WL 3653173, at *19 (D. Colo. Aug. 1, 2018) ("Defendant is correct California . . . do[es] not recognize a separate cause of action for negligence per se. In [California], alleged violations of safety statutes are simply evidence of negligence." (citations omitted)), report and recommendation adopted in part, rejected in part on other grounds, 344 F. Supp. 3d 1231 (D. Colo. 2018); In re Kaplan, No. 3:11-CV-00772-RCJ, 2011 WL 6140683, at *2 (D. Nev. Dec. 9, 2011) ("Negligence per se is not a separate cause of action but a doctrine whereby the floor for the duty of care is set as a matter of law, taking away from the fact-finder the "reasonable person" determination and leaving to the fact-finder only a determination of causation and damages. . . ." (citing Ashwood v. Clark Cty., 930 P.2d 740, 743–44 (Nev. 1997))); Johnson v. Enriquez, 460 S.W.3d 669, 673 (Tex. App. 2015) ("Negligence per se is not a separate cause of action independent of a common-law negligence cause of action. Rather, negligence per se is merely one method of proving a breach of duty. . . ." (citations omitted)).

Plaintiffs have not shown they conferred a benefit upon Brinker, or that Brinker knew Plaintiffs were conferring a benefit.

In merchant-consumer transactions, courts have developed two theories for determining if a consumer has conferred a benefit on the merchant: (1) the "overpayment" theory; and (2) the "would not have shopped" theory. The "overpayment" theory is when customers pay in excess of what the good or service was worth, with that excess considered a "benefit" to the merchant if the customer did not receive what they fully expected. Resnick, 693 F.3d 1317. In Resnick, the customers alleged they conferred a monetary benefit upon the defendant, a company selling health care plans, in the form of monthly premiums that included a portion allocated to data security. Id. at 1328. The court denied the defendant's motion to dismiss the unjust enrichment claim because the defendant failed to keep the plaintiffs' data secure. Id. However, no court has extended this theory to data breach cases outside of the healthcare context. In re Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1178 (D. Minn. 2014) (distinguishing Resnick on the grounds that every customer in Resnick was at risk from insufficient security because every customer had to provide their confidential information to purchase the health care plans). In a normal consumer transaction (like the ones at issue here), the price is the same regardless of the payment method, yet only customers using payment cards are at risk of having their personal data compromised. Id. Thus, because the

customers must have paid only what the good or service was worth, and nothing more, they conferred no additional benefit upon the defendant. Irwin v. Jimmy John's Franchise, LLC, 175 F. Supp. 3d 1064, 1072 (C.D. Ill. 2016); Brush, 238 F. Supp. 3d at 1369.

Plaintiffs allege they purchased goods and services from Brinker, and in exchange they "should have received from Brinker the goods and services that were the subject of the transaction and should have been entitled to have Brinker protect their Customer data with adequate data security." (Doc. 39 ¶ 190). Similar to Target, this case is not controlled by Resnick because there are no allegations that every customer, regardless of payment method, required data security. See Target, 66 F. Supp. 3d at 1178. Because card-paying customers did not pay more than cash customers for Brinker's goods and services the overpayment theory fails. See id.; (Doc. 39).

The "would not have shopped" theory is where a customer would not have purchased the good or service had they been fully informed about it, and, thus, the merchant is not entitled to the money it received. Target, 66 F. Supp. 3d at 1177-78 (applying Minnesota unjust enrichment law which requires a plaintiff plead facts showing the defendant knowingly received or obtained something of value they "in equity and good conscience" should not have received). The plaintiffs in Target pled that they shopped at Target after Target knew, or should have known, about the data breach, and that they would not have

shopped there had they been informed of the breach. Id. The court held a reasonable jury could conclude that the money the customers spent is money that Target "in equity and good conscience" should not have received because if it informed the plaintiffs of the data breach, they would not have spent money there. Id.

However, the "would not have shopped" theory is unpersuasive here. Like Target, Plaintiffs allege that if they "knew that Brinker would not secure their Customer data using adequate security, they would not have made purchases" at Brinker's locations. (Doc. 39 ¶ 194). However, unlike Target, Plaintiffs never allege Brinker knew about the breach at the time Plaintiffs were dining at Chili's. (Doc. 39). Further, Target appears to be an outlier among data breach cases in recognizing the "would not have shopped" theory, which is likely attributable to the unique circumstance that Target allegedly knew about the breach as it was ongoing. See, e.g., Gordon, 344 F. Supp. 3d at 1249; In re Zappos.com, Inc., No. 3:12-CV-00325-RCJ, 2013 WL 4830497, at *4 (D. Nev. Sept. 9, 2013) (applying Nevada law in data breach action and dismissing the unjust enrichment claims). Overall, Plaintiffs have not shown that they conferred a benefit upon Brinker.

Plaintiffs have also not shown that Brinker knew they were conferring a benefit, that Brinker accepted the benefit, or that it is inequitable for Brinker to retain the benefit. Resnick, 693 F.3d at 1328. Plaintiffs allege only conclusory

statements regarding Brinker's knowledge and acceptance of the benefit. (Doc. 39 ¶ 191). The Complaint states, "Brinker knew that Plaintiffs and Class members conferred a benefit on Brinker and accepted or retained that benefit," and that Brinker "profited from the purchases and used the Customer data . . . for business purposes." (Doc. 39 ¶ 191). However, there are no factual allegations supporting these elements. Thus, the unjust enrichment claim must be dismissed. See, e.g., Irwin, 175 F. Supp. 3d at 1072 ("Irwin paid for food products. She did not pay for a side order of data security and protection; it was merely incident to her food purchase. . . . Irwin does not allege that she paid more than cash customers did for the same food items, so it cannot be said that Jimmy John's was unjustly enriched by her purchases.").

E. Declaratory Judgment (Count V)

Count V of the complaint seeks a declaration that: (a) Brinker's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Brinker must implement and maintain reasonable security measures . . . ." (Doc. 39 ¶ 205). Plaintiffs then list eight measures they wish the Court to impose on Brinker. It is unclear under what legal authority this count is brought.

Brinker makes two arguments related to Count V. First, it contends that "Declaratory relief is a procedural device which depends on an underlying

substantive cause of action and cannot stand on its own[;]" because the Court should dismiss Counts I–IV, it should dismiss Count V as well. (Doc. 48 at 37 (quoting Eveillard v. Nationstar Mortg. LLC, No. 14-CIV-61786, 2015 WL 127893, at *9 (S.D. Fla. Jan. 8, 2015)). Second, Brinker argues that the declaratory relief claim should be dismissed because it is duplicative of the other claims alleged in the complaint. Plaintiffs assert that Counts I–IV have been adequately pled, and that "although Plaintiffs seek a declaration stating that Defendant did not comply with its contractual obligations and duties of care, Plaintiffs also request a declaration stating the reasonable security measures that Defendant must implement in order to comply with said obligations and duties." (Doc. 53 at 31).

The first portion of the declaratory relief claim should be stricken, as Plaintiffs implicitly acknowledge. Whether Brinker breached its implied contract or duties of care are contained in Counts I–IV. However, Plaintiffs also seek prospective relief requiring Brinker to safeguard Plaintiffs' data that Brinker still possesses. District courts have ruled inconsistently on this issue. In Irwin, the court dismissed the declaratory judgment count because the plaintiff "[did] not allege that the data breach exposed information that continues to pose a risk that is certainly impending, or presents a substantial risk of future harm." Irwin, 175 F. Supp. 3d at 1073–74. Essentially, the court determined that the plaintiff did not have standing under the Declaratory

Judgment Act because the likelihood of another data breach was merely possible, not actual or imminent. Id. However, in In re: The Home Depot, Inc., Customer Data Sec. Breach Litig., No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *4 (N.D. Ga. May 18, 2016), the court refused to dismiss the plaintiffs' claim for declaratory relief based on future harm.[12]

Plaintiffs allege that their data is more vulnerable than before because Brinker's lax security has become public. (Doc. 39 ¶ 203). Further, Plaintiffs allege the prevalence of data breaches and that Brinker has done nothing to secure its systems. However, Plaintiffs have also alleged that they obtained new cards. (Doc. 39 ¶¶ 29, 30, 45, 48–49). Thus, even if Brinker's systems remain insecure and still contain Plaintiffs' old card data, Plaintiffs do not face a risk of future harm that is more than possible. Count V is due to be dismissed.[13]

F. FDUTPA (Count VI)

"[A] consumer claim for damages under FDUTPA has three elements: (1) a deceptive act or unfair practice; (2) causation; and (3) actual damages."

[12] The court did dismiss the portion of the claim seeking a declaration that the defendant had breached its duty because it related to past liability that was covered under the plaintiffs' negligence claims. Id.

[13] If Plaintiffs decide to replead the Declaratory Judgment claim based on future harm, they should also file a supplemental brief addressing the Court's concerns.

Rollins, Inc. v. Butland, 951 So. 2d 860, 869 (Fla. 2d DCA 2006). Brinker contends that Plaintiffs failed to allege an unfair practice and damages.

"An unfair practice is 'one that offends established public policy and one that is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers.'" PNR, Inc. v. Beacon Prop. Mgmt., Inc., 842 So. 2d 773, 777 (Fla. 2003) (quoting Samuels v. King Motor Co. of Ft. Lauderdale, 782 So. 2d 489, 499 (Fla. 4th DCA 2001)). In determining whether an act is an unfair practice, "due consideration and great weight shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to [§] 5(a)(1) of the Federal Trade Commission Act, 15 U.S.C. [§] 45(a)(1). . . ." § 501.204, Fla. Stat. (2018).

At least one district court within the Eleventh Circuit has found a FDUTPA violation for failure to secure personal information. Burrows v. Purchasing Power, LLC, No. 1:12-CV-22800-UU, 2012 WL 9391827, at *6 (S.D. Fla. Oct. 18, 2012) ("Burrows's first FDUTPA allegation, that Defendants failed to adequately secure his PII, qualifies as an unfair practice."). And, several courts have determined that the failure to maintain reasonable and appropriate data security for sensitive personal information violates the FTC Act. E.g., F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 247 (3d Cir. 2015) (finding that lax cybersecurity resulting in a data breach of customer information could fall within the meaning of "unfair" under the FTCA); In re Equifax, Inc.,

Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1327 (N.D. Ga. 2019) ("The failure to maintain reasonable and appropriate data security for consumers' sensitive personal information can constitute an unfair method of competition in commerce in violation of the Federal Trade Commission Act.").

Because Plaintiffs allege that Brinker violated the FTC Act by providing inadequate security for customer data, they have alleged an unfair practice. (Doc. 39 ¶¶ 210–11). Brinker's argument that Plaintiffs failed to allege any facts demonstrating how its systems were inadequate is unpersuasive. (Doc. 48 at 37–38). Plaintiffs allege that Brinker failed to "properly secure and protect payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; protect systems against malware; regularly test security systems; establish a process to identify and timely fix security vulnerabilities; and encrypt payment card data at the point of sale." (Doc. 39 ¶ 88). These allegations demonstrate how Brinker's systems were inadequate.

Brinker next argues that Plaintiffs have no "legally cognizable damages." (Doc. 48 at 38). Green-Cooper (the Florida Statewide Class representative) alleges that she suffered fraudulent charges on her credit card, lost the ability to accrue cash back rewards, lost time monitoring her accounts and contacting her bank, and overpaid for Chili's goods and services. (Doc. 53 at 33).

Any person "who has suffered a loss as a result of a violation of [FDUTPA] . . . may recover actual damages, plus attorney's fees and court costs . . . ." § 501.211(2), Fla. Stat. (2018). However, FDUTPA does not apply to "[a] claim for personal injury or death or a claim for damage to property other than the property that is the subject of the consumer transaction." § 501.212(3), Fla. Stat. (2018). The statute does not define the term "property," but "[Florida District Courts of Appeal] have held that section 501.211 'entitles a consumer to recover damages attributable to the diminished value of the goods or services received, but does not authorize recovery of consequential damages to other property attributable to the consumer's use of such goods or services.'" Schauer v. Morse Operations, Inc., 5 So. 3d 2, 6 (Fla. 4th DCA 2009) (quoting Ft. Lauderdale Lincoln Mercury, Inc. v. Corgnati, 715 So. 2d 311, 314 (Fla. 4th DCA 1998)).

Consequential damages are "losses that do not flow directly and immediately from an injurious act but that result indirectly from the act." *Consequential Damages*, Black's Law Dictionary (11th ed. 2019). In Schauer, the court found that damages to the plaintiff's credit rating based on being fraudulently told that he would not be obligated to repay a loan for which he cosigned, were consequential, and thus, unrecoverable. Schauer, 5 So. 3d at 6. Similarly, loan payments, interest, and a down payment in purchasing a watercraft are not "actual damages" after the watercraft unexpectedly caught

fire and sank. Rodriguez v. Recovery Performance & Marine, LLC, 38 So. 3d 178, 181 (Fla. 3d DCA 2010) (stating that the correct measure of damages is the difference in market value as delivered from the market value as it should have been delivered).

Here, Plaintiffs have not alleged damages recognized under FDUTPA because unauthorized charges, lost time, and lost cash-back rewards are all consequential damages. See Rodriguez, 38 So. 3d at 181; Schauer, 5 So. 3d at 6. Plaintiffs' allegation that they "overpaid for the goods and services provided by Defendant because they would not have dined at Chili's had Defendant disclosed its inadequate data security" also fails. (Doc. 53 at 33). The "property that is the subject of the consumer transaction" is the food or drinks that Plaintiffs purchased. § 501.212(3). In the same way that loan payments and interest are consequential costs of financing the purchase of a car or boat, so to is data security for payment information in purchasing food at a restaurant using a credit card. See Rodriguez, 38 So. 3d at 181; Schauer, 5 So. 3d at 6. Ultimately, the food or drink purchased has no diminished value because of Brinker's alleged inadequate data security; Plaintiffs' personal information is merely "other property" that was damaged as a result of purchasing food or drinks from Brinker. See Corgnati, 715 So. 2d at 314 ("[FDUTPA] entitles a consumer to recover damages attributable to the diminished value of the goods or services received, but does not authorize recovery of consequential damages

to other property attributable to the consumer's use of such goods or services." (quoting Urling v. Helms Exterminators, Inc., 468 So. 2d 451, 454 (Fla. 1st DCA 1985))). Because Plaintiffs have failed to allege damages recognized under FDUTPA, Count VI is due to be dismissed.[14]

G. Texas Trade Practices (Count VII)

Brinker argues that Plaintiffs fail to state a claim for a violation of the Texas DTPA. The Texas DTPA states:

> (a) A consumer may maintain an action where any of the following constitute a producing cause of economic damages or damages for mental anguish:
>
> (1) the use or employment by any person of a false, misleading, or deceptive act or practice that is:
>
> (A) specifically enumerated in a subdivision of Subsection (b) of Section 17.46 of this subchapter; and
>
> (B) relied on by a consumer to the consumer's detriment; [or]
>
> . . . .
>
> (3) any unconscionable action or course of action by any person;

Tex. Bus. & Com. Code § 17.50 (2019). Brinker does not dispute that Shenika Thomas (the Texas Statewide Class representative) and the Texas class members are consumers. Plaintiffs allege three violations enumerated in § 17.46(b): "(5) representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not

[14] If Plaintiffs contest this view of FDUTPA damages law, they may file a supplemental brief in support of their Third Amended and Consolidated Complaint.

have[;]" "(7) representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another;" and "(9) advertising goods or services with intent not to sell them as advertised." See (Doc. 39 ¶ 223). Further, Plaintiffs allege that Brinker's inadequate data security was an unconscionable action, violating § 17.50(a)(3).

Plaintiffs allege no facts supporting any express representation or advertisement by Brinker, which is required for a violation of § 1746(b)(5), (7), and (9).[15] See Dyer v. Danek Med., Inc., 115 F. Supp. 2d 732, 740 (N.D. Tex. 2000) (granting summary judgment for defendants on DTPA claims because the plaintiffs failed to present any evidence of representations made; allegations of a failure to disclose were insufficient); cf. In re Zappos.com, 2013 WL 4830497, at *7 ("Plaintiffs have sufficiently alleged false, misleading, or deceptive practices [under the Texas DTPA] via the statements on Zappos's website that

[15] It is possible that Plaintiffs intended that Brinker's 10-K be the affirmative representations required under the Texas DTPA (or the California equivalent discussed below). However, Plaintiffs discussion of the 10-Ks and the statements related to technology within them do not support a deceptive practice claim. First, Plaintiffs did not allege that they relied upon the 10-K as a representation that their data would be secure. Second, a 10-K is information presented to shareholders and potential investors, not advertisements for Chili's or Maggiano's (Brinker's other restaurant chain). Thus, it is not plausible to infer that a customer of Chili's would rely on statements made in its parent company's 10-K as a reason to dine at Chili's and believe that payment card information would be kept secure. Generally, it is not unreasonable to assume that a company accepting credit or debit cards has some level of security to keep payment card data safe. However, that belief is not based on what a company says in its 10-K.

Plaintiffs' personal data was secure."). Instead, Plaintiffs make only conclusory allegations that Brinker violated the Texas DTPA, which are insufficient to state a claim for relief under Rule 8. See Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (requiring sufficient factual content to make a claim plausible on its face).

For a representation to be implied under the Texas DTPA, it must have been "clearly contemplated by the party charged with making it." Red Roof Inns, Inc. v. Jolly, No. 14-10-00344-CV, 2011 WL 6288147, at *4 (Tex. App. Dec. 15, 2011) (finding that having a security guard in a hotel lobby was not an implied representation that the hotel was secure). "A representation should be implied from conduct only when, under the circumstances at the time the party engaged in that conduct, the only reasonable interpretation of that conduct is that the party meant to convey the representation in question." Id. Further:

> To qualify as an implied representation, the representation must be so obvious that it did not need to be stated. More importantly, there must be one and only one thing that the implied representation reasonably could mean. The law will not imply a representation when a party is said to have represented one thing by its conduct and the same action or conduct reasonably could be construed to have a different meaning.

Id. at *5. Plaintiffs have not identified any conduct by Brinker that would satisfy this standard for an implied representation under the Texas DTPA. See id. Further, in the same way that a hotel's maintaining a security guard in the lobby, providing separate keys for each room, and not providing safes for guests

is not an implied representation that the hotel is safe, accepting credit cards as a form of payment is also not an implied representation that the payment card information would be kept secure. Id. Thus, as currently pled, Plaintiffs have not alleged a Texas DTPA violation under § 17.50(1).

Plaintiffs also allege that Brinker violated § 17.50(3) of the Texas DTPA by engaging in unconscionable acts. (Doc. 39 ¶ 229). Under the Texas Business and Commercial Code, an "'[u]nconscionable action or course of action' means an act or practice which, to a consumer's detriment, takes advantage of the lack of knowledge, ability, experience, or capacity of the consumer to a grossly unfair degree." Tex. Bus. & Com. Code § 17.45(5) (2019). "Unconscionability under the DTPA is an objective standard for which scienter is irrelevant. To prove an unconscionable action or course of action, a plaintiff must show that the defendant took advantage of his lack of knowledge and 'that the resulting unfairness was glaringly noticeable, flagrant, complete and unmitigated.'" Bradford v. Vento, 48 S.W.3d 749, 760 (Tex. 2001) (quoting Ins. Co. of N. Am. v. Morris, 981 S.W.2d 667, 677 (Tex. 1998)).

Plaintiffs state only conclusory allegations to support their claim that Brinker's acts were unconscionable. Paragraphs 229 through 231 of the complaint do nothing more than add in party names to the elements without any factual underpinnings to support those allegations. See Iqbal, 556 U.S. at 678. If the complaint alleges specific facts demonstrating an objective

unconscionable action that was the producing cause of their injuries, then Plaintiffs should have cited those allegations in their response to the motion to dismiss. Their citation to paragraph 229 as support is insufficient.[16] Accordingly, Count VII will be dismissed.

H. California's Unfair Competition Law (Counts X, XI, and XII)

The UCL prohibits unfair competition, which it defines as "any unlawful, unfair or fraudulent business act or practice." Kwikset Corp. v. Superior Court, 246 P.3d 877, 883 (Cal. 2011). Its purpose is "to protect both consumers and competitors by promoting fair competition in commercial markets for goods and services." Id. To that end, the California legislature framed the UCL's substantive provisions in "broad, sweeping language and provided courts with broad equitable powers to remedy violations." Id. (citations and quotations omitted). "Remedies for private individuals bringing suit under the UCL are limited to restitution and injunctive relief." In re Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953, 984 (N.D. Cal. 2016) (quoting Pom Wonderful LLC v. Welch Foods, Inc., 2009 WL 5184422, *2 (C.D. Cal. Dec. 21, 2009)).

[16] Paragraph 229 states in full: "Brinker engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Brinker engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree."

1. Standing under California's UCL.

Under the UCL, "standing is limited to any 'person who has suffered injury in fact and has lost money or property' as a result of unfair competition." Kwikset, 246 P.3d at 884 (quoting § 17204, as amended by Prop. 64, as approved by voters, Gen. Elec. (Nov. 2, 2004) § 3). The injury in fact requirement is the same as that required by Article III in federal court. Id. at 885. However, under the UCL a plaintiff must also show economic injury. Id. Economic injury from unfair competition can be shown in innumerable ways; in a non-exhaustive list the California Supreme Court provided examples:

> A plaintiff may (1) surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of money or property to which he or she has a cognizable claim; or (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary.

Id. at 885–86. In cases where the UCL claim is premised on a misrepresentation (as here), "a plaintiff must show that the misrepresentation was an immediate cause of the injury-producing conduct." Id. at 888 (quotation marks omitted) (quoting In re Tobacco II Cases, 207 P.3d 20, 39 (Cal. 2009)).

A consumer can satisfy the UCL's standing requirements by alleging that they would not have purchased a product but for a misrepresentation. Id. at 890. "[B]ecause of the misrepresentation the consumer (allegedly) was made to part with more money that he or she otherwise would have been willing to

expend. . . . That increment, the extra money paid, is economic injury and affords the consumer standing to sue." Id. at 890–91. The plaintiff would not need to prove that the item purchased was worth less, only that they would not have purchased it but for the misrepresentation. Id. at 894.

Here, Plaintiffs allege that they would not have dined at Chili's had they known it had inadequate data security. (Doc. 39 ¶ 50). This is sufficient for standing under the UCL. Kwikset, 246 P.3d at 890–91; see also Gordon, 2018 WL 3653173, at *27 (finding standing under the UCL because plaintiffs alleged they relied on defendant's omission that it was not providing reasonable data security, such information was material, and had they known the truth plaintiffs would not have made the purchases).

2. The UCL's unlawful prong (Count X).

To state a cause of action based on an unlawful business act or practice under the UCL, a plaintiff must sufficiently allege a violation of some underlying law. People v. McKale, 602 P.2d 731, 735 (Cal. 1979). Violation of almost any law can serve as the basis for a UCL claim. In re Anthem, 162 F. Supp. 3d at 989. The claim must identify the specific section of a statute that was violated and must describe with reasonable particularity the facts supporting the violation. Baba v. Hewlett-Packard Co., No. C 09-05946 RS, 2010 WL 2486353 at *6 (N.D. Cal. June 16, 2010). Plaintiffs allege violations of the FTC Act and California Civil Code §§ 1798.81.5 and 1798.82.

i. Plaintiffs have alleged a violation of the FTC Act.

Plaintiffs allege that Brinker violated the FTC Act by employing sub-standard security practices and soliciting and collecting Plaintiffs' personal information "with knowledge that the information would not be adequately protected." (Doc. 39 ¶ 261). Plaintiffs allege that had Brinker disclosed that its security was inadequate they would not have dined at Chili's or would not have paid with a card. Plaintiffs have alleged an unfair practice under the FTC Act.

ii. Plaintiffs have alleged a violation of California Civil Code § 1798.81.5.

Plaintiffs also allege liability under the UCL's unlawful prong via violations of California Civil Code § 1798.81.5, which requires that a business "implement and maintain reasonable security procedures and practices appropriate to the nature of the information." Cal. Civ. Code § 1798.81.5. To that end, Plaintiffs cite various industry guidelines and recommendations that Brinker allegedly knew of but unreasonably failed to implement. (Doc. 39 ¶ 81–98).

Failure to take reasonable data security precautions constitutes a violation of § 1798.81.5. Where the plaintiffs allege a failure to implement and maintain reasonable security procedures and an injury caused by those failures,

they have sufficiently pled a violation of § 1798.81.5. E.g., Hameed-Bolden v. Forever 21 Retail, Inc., No. CV1803019SJOJPRX, 2018 WL 6802818, at *7 (C.D. Cal. Oct. 1, 2018); In re Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1226 (N.D. Cal. 2014). However, plaintiffs must do more than allege that the defendant knew of better security protocols and failed to implement them. Razuki v. Caliber Home Loans, Inc., No. 17CV1718-LAB (WVG), 2018 WL 6018361, at *1 (S.D. Cal. Nov. 15, 2018). In Razuki, the plaintiffs argued that the defendant knew of higher-quality security protocols available to it but failed to implement those measures. Razuki, 2018 WL 6018361 at *2. The court dismissed the claim because the plaintiffs had not alleged any facts showing that the defendant did not live up to industry standards. Id. However, the court noted that the claim would have survived had the plaintiffs "identified what made [the defendant]'s security measures unreasonable by comparison to what other companies are doing, but simply knowing of higher-quality security measures is not sufficient to state a claim." Id.

Here, Plaintiffs allege that Brinker's data security was unreasonable and identify specific security standards it should have implemented. (Doc. 39 ¶ 83–90). Unlike in Razuki, Plaintiffs allege that Brinker employed sub-industry-standard security measures at the time of the data breach and make direct mention of specific security measures Brinker should have taken (such as point-to-point and end-to-end encryption). See id.; (Doc. 39 ¶¶ 90, 98); see also Dugas

v. Starwood Hotels & Resorts Worldwide, Inc., No. 3:16-CV-00014-GPCBLM, 2016 WL 6523428, at *7 (S.D. Cal. Nov. 3, 2016) (finding allegations that the defendant failed to appropriately encrypt customers' data sufficient to state a claim under § 1798.81.5). Thus, Plaintiffs have stated a claim under the unlawful prong of the UCL via violations of § 1798.81.5.

iii. Plaintiffs fail to allege a violation of California Civil Code § 1798.82

Plaintiffs' final unlawful prong claim is premised on alleged violations of California Civil Code § 1798.82, which outlines notification requirements for businesses subjected to a data breach. § 1798.82. California law requires that a business notify its customers of a data breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82(a). There is no proscribed length of time between discovering a data breach and informing those affected so long as any delay in notification is reasonable. Razuki, 2018 WL 6018361 at *2. In Razuki, the defendants waited five months to notify the plaintiffs, but the court dismissed the claim because plaintiffs had not alleged that such delay was unreasonable. Id.

Additionally, § 1798.82 dictates what information must be provided, the format in which the information must be presented, and the manner of conveyance. § 1798.82. In alleging a violation of § 1798.82, Plaintiffs must show that the delay in notification or incorrect or incomplete information caused

some additional harm. Starwood Hotels, 2016 WL 6523428, at *7 ("[B]ecause Plaintiff has failed to trace any harm from Defendants' delayed notification or to demonstrate a nexus between the alleged harm flowing from the delayed notification and Defendants' actions, Plaintiff has failed to adequately allege[] causation with respect to his CRA § 1798.82 claim.").

Brinker argues that this Count should be dismissed because it notified Plaintiffs one day after it discovered the breach, and that Plaintiffs failed to allege damages caused by any such delay. (Doc. 48 at 43). Plaintiffs respond that they do not agree with Brinker's timeline of events, that they need discovery to determine if Brinker complied with the manner and means of the notice requirement, and that at least some "damages can be traced to delay: had Defendant given notice of the Breach earlier, Plaintiffs could have taken mitigation steps." (Doc. 53 at 39–40).

Plaintiffs fail to state an unlawful UCL claim premised on a violation of § 1798.82. First, despite Plaintiffs' argument that they disagree with Brinker's timeline, the timeline is based on the allegations in the complaint. Plaintiffs allege that the breach began in March 2018, and Brinker publicized the breach on May 12, 2018. (Doc. 39 ¶¶ 101–02). Plaintiffs do not allege that Brinker knew about the breach earlier than May 11, 2018 (the date Brinker claims it learned of the breach) and no reasonable inference can be drawn supporting Plaintiffs'

unsubstantiated argument that Brinker may have known about the breach earlier. (Doc. 53 at 36).

Second, Plaintiffs' allegation that Brinker did not provide timely and accurate information is refuted by other allegations. (Doc. 39 ¶ 266). Assuming Brinker was entitled to use substitute notice (Plaintiffs have not alleged they were not entitled to such), Brinker's online posting satisfies all of the content requirements set forth in § 1798.82(d)(2).[17] See § 1798.82(d)(2); (Doc. 39 ¶ 102). Further, Plaintiffs allege that Brinker sent email notices to at least some affected individuals. (Doc. 39 ¶ 36, 38, 40). Lastly, Plaintiffs have failed to allege damages caused by the untimely or incomplete notification. Plaintiffs do not allege what injuries they suffered as a result of their inability to take mitigation steps in the one-day period before Brinker published its notice. See Adobe, 66 F. Supp. 3d at 1217 (dismissing a UCL claim predicated on California Civil Code § 1798.82 because Plaintiffs failed to allege suffering incremental harm as a result of the delay). Therefore, Plaintiffs have failed to allege a violation of § 1798.82.

[17] The online announcement of the breach was originally published on May 12, 2018, the day after Brinker claims it learned of the breach. The website, which is provided in the complaint, states that it was updated on September 20, 2018. It is unclear if the original posting contained all of the necessary information. However, Plaintiffs have failed to allege what information was lacking.

Thus, Brinker's motion to dismiss Plaintiffs unlawful prong UCL claim is denied insofar as it alleges underlying violations of the FTC Act and California Code § 1798.81.5, but granted to the extent Plaintiffs' unlawful prong UCL claim is premised on § 1798.82.

3. The UCL's unfair prong (Count XI).

The unfair prong prohibits competitive practices that, although not proscribed by specific law, are nonetheless unfair. See Cel-Tech Commc'ns, Inc., v. L.A. Cellular Tel. Co., 973 P.2d 527, 560–63 (Cal. 1999). "The standard for determining what business acts or practices are 'unfair' in consumer actions under the UCL is currently unsettled." Zhang v. Superior Court, 304 P.3d 163, 174 n.9 (Cal. 2013). Three separate tests have emerged: the balancing test, the tethering test, and the FTC Act test. Id.; see also MacDonald v. Ford Motor Co., 37 F. Supp. 3d 1087, 1098–99 (N.D. Cal. 2014) (explaining the different "unfair" tests used by California courts). Here, Plaintiffs' claim survives under all three tests, but the Court need only analyze the tethering test to see why.

In Cel-Tech, the California Supreme Court applied a tethering test, proclaiming that unfairness must be "tethered to some legislatively declared policy or proof of some actual or threatened impact on competition." Cel-Tech, 973 P.2d 527 at 561. In Adobe, the court noted that to survive the tethering test, a plaintiff need only show that the effects of the defendant's conduct are comparable to or the same as a violation of the law." 66 F. Supp. 3d at 1227. As

Plaintiffs' unlawful prong claim based on violations of the FTC Act and § 1798.81.5 survives, so too, does their unfair claim because the effects of Brinker's conduct are the same as under a violation of the law. See Adobe, 66 F. Supp. 3d at 1227.

4. The UCL's fraudulent business act or practice prong (Count XII).

The fraudulent prong is governed by the reasonable consumer test: "a plaintiff may demonstrate a violation by 'show[ing] that [reasonable] members of the public are likely to be deceived.'" Rubio v. Capital One Bank, 613 F.3d 1195, 1204 (9th Cir. 2010) (quoting Williams v. Gerber Prods. Co., 552 F.3d 934, 938 (9th Cir. 2008)). The deception does not need to be intentional. Id. Claims under the fraud prong are subject to the particularity requirements of Rule 9(b). Kearns v. Ford Motor Co., 567 F.3d 1120, 1125 (9th Cir. 2009).

Plaintiffs allege that Brinker made both misrepresentations and omissions that satisfy the fraud prong. As discussed previously under Texas's consumer protection laws, Plaintiffs fail to identify any representation by Brinker. However, omissions of material facts are actionable under the fraud prong if the defendant had a duty to disclose. In re Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2017 WL 3727318, at *2 (N.D. Cal. August 30, 2017). There are four circumstances giving rise to a duty to disclose: "(1) when the defendant is the plaintiff's fiduciary; (2) when the defendant has exclusive knowledge of a material fact not known or reasonably accessible to

the plaintiff; (3) when the defendant actively conceals a material fact from the plaintiff; [or] (4) when the defendant makes partial representations that are misleading because some other material fact has not been disclosed." Id. (quoting Collins v. eMachines, Inc., 134 Cal. Rptr. 3d 588, 593 (Cal. Ct. App. 2011)). A fact is material if a reasonable consumer would deem it important in determining how to act in the transaction at issue. Collins, 134 Cal. Rptr. 3d at 593.

Plaintiffs allege that they would not have dined at Chili's had they known Brinker's data security failed to comply with industry standards. (Doc. 39 ¶¶ 50, 295). In their response, Plaintiffs argue that "Defendant had a duty to disclose its inadequate data security because it had exclusive knowledge of these facts, and these facts were material." (Doc. 53 at 41). Absent from this assertion is a citation to factual allegations in the complaint that support it. Thus, Plaintiffs fail to allege a basis for Brinker's duty to disclose. It could be inferred that Brinker had exclusive knowledge that its data security was inadequate, but under Rule 9(b) allegations of fraudulent omission require particularity. Fed. R. Civ. P. 9(b). Further, in their Texas DTPA claim, Plaintiffs allege (albeit in conclusory fashion) that Brinker had a duty to disclose. (Doc. 39 ¶ 228). Thus, Plaintiffs have failed to allege a violation of the UCL's fraudulent prong.

I. Nevada Consumer Fraud Act (Count XII(b))

Plaintiffs allege that Brinker violated the Nevada CFA, Nev. Rev. Stat. § 41.600, by engaging in consumer fraud. Section 41.600(2) defines "consumer fraud" by reference to other statutes. Specific to this case, § 41.600(2)(e) makes it unlawful to engage in a deceptive trade practice defined in Nevada Revised Statutes §§ 598.0915 through 598.0925. Plaintiffs allege that Brinker engaged in conduct defined in §§ 598.0917(7), 598.0923(3), 603A.210, and 603A.215.

Plaintiffs' first claim that Brinker committed consumer fraud by engaging in a deceptive trade practice defined in § 598.0917(7) fails. That section defines a deceptive trade practice as:

> A person engages in a "deceptive trade practice" when in the course of his or her business or occupation he or she employs "bait and switch" advertising, which consists of an offer to sell or lease goods or services which the seller or lessor in truth may not intend or desire to sell or lease, accompanied by one or more of the following practices:
>
> . . . .
>
> 7. Tendering a lease of goods advertised for sale or a sale of goods advertised for lease or tendering terms of sale or lease less favorable than the terms advertised

Nev. Rev. Stat. § 598.0917 (2019). Plaintiffs have not sufficiently alleged this cause of action. They selectively quote the statute, which fundamentally changes the definition of a deceptive trade practice. Plaintiffs claim that they need only show that Brinker tendered terms of sale less favorable than those advertised. But this is not true: Plaintiff must allege both that the seller offered

goods or services that it did not in truth intend to sell and that it tendered the goods or services on less favorable terms than advertised. "Described more colloquially, [bait-and-switch] is a 'sales practice whereby a merchant advertises a low-priced product to lure customers into the store only to induce them to buy a higher-priced product.'" Rimini St., Inc. v. Oracle Int'l Corp., No. 2:14-CV-1699-LRH-CWH, 2017 WL 5158658, at *10 (D. Nev. Nov. 7, 2017) (quoting Black's Law Dictionary). Plaintiff makes no allegations that Brinker engaged in a bait and switch or that it made any advertisement with terms more favorable than to those received. Therefore, Plaintiffs fail to allege a violation of § 598.0917(7).

Plaintiffs next allege that Brinker committed a deceptive trade practice by "violat[ing] a state or federal statute or regulation relating to the sale or lease of goods or services." Nev. Rev. Stat. § 598.0923(3) (2019). Plaintiffs allege that Brinker violated §§ 603A.210 and 603A.215. Section 603A.210 requires any business that collects personal information to maintain reasonable security of that information, and § 603A.215 requires:

> If a data collector doing business in this State accepts a payment card in connection with a sale of goods or services, the data collector shall comply with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council or its successor organization, with respect to those transactions, not later than the date for compliance set forth in the Payment Card Industry (PCI) Data Security Standard or by the PCI Security Standards Council or its

successor organization.

Nev. Rev. Stat. § 603A.215 (2019). Plaintiffs have sufficiently alleged violations of these sections. Brinker is alleged to be a "data collector" under the statute, see § 603A.030; (Doc. 39 ¶ 64), and it is alleged that Brinker failed to comply with the PCI Data Security Standards, (Doc. 39 ¶ 90).

Brinker argues that Plaintiffs must allege that the data breach was the result of Brinker's intentional conduct or gross negligence. (Doc. 48 at 47 (citing § 603A.215(3)(b))). But Brinker is incorrect. Employing similar tactics as Plaintiffs, Brinker selectively quotes the portion of the statute that helps them. Section 603A.215(3) states: "A data collector shall not be liable for damages for a breach of the security of the system data if: (a) The data collector is in compliance with this section; and (b) The breach is not caused by the gross negligence or intentional misconduct of the data collector, its officers, employees or agents." § 603A.215(3) (emphasis added). Contrary to Brinker's assertion, Plaintiffs do not need to allege that it was grossly negligent because Plaintiffs sufficiently allege that Brinker was not in compliance with the PCI DSS. (Doc. 39 ¶¶ 85–90).

Brinker also argues that Plaintiffs' Nevada CFA claim should be dismissed for failure to allege "legally cognizable damages." (Doc. 48 at 47). Brinker does not state what types of damages are "legally cognizable" under the Nevada CFA, and case law is unclear. Recently, one federal district court found

that a plaintiff failed to plead sufficient damages under the Nevada CFA, finding "Plaintiffs' damages, if any, were economic in nature, as they have not alleged personal injury or property damage." Ames v. Caesars Entm't Corp., No. 217CV02910GMNVCF, 2019 WL 1441613, at *3 (D. Nev. Apr. 1, 2019). However, the statute states that if the claimant prevails, she is entitled to "any damages that the claimant has sustained. . . ." § 41.600(3)(a). Other courts have found that non-personal injury or property damage claims can survive. Cf. Bauman v. Saxe, No. 2:14-CV-01125RFBPAL, 2019 WL 591439, at *4 (D. Nev. Feb. 13, 2019) (finding that plaintiffs plausibly pled damages in the form of "privacy violations and a disruption in the quiet use and enjoyment of their cellular telephones."). Thus, under the more expansive definition of damages, which comports with the plain text of the statute, Plaintiffs have sufficiently alleged damages under the Nevada CFA.

Accordingly, the portion of Count XII(b) premised on violations of § 598.0917(7) will be dismissed but the rest of the count remains.

J. Breach of Confidence (Count XIII)

"A common law breach of confidence lies where a person offers private information to a third party in confidence and the third party reveals that information." Muransky v. Godiva Chocolatier, Inc., 922 F.3d 1175, 1190–91 (11th Cir. 2019) (citing Alan B. Vickery, Breach of Confidence: An Emerging Tort, 82 Colum. L. Rev. 1426, 1427–28 (1982); and Alicia Solow-

Niederman, Beyond the Privacy Torts: Reinvigorating A Common Law Approach for Data Breaches, 127 Yale L.J. Forum 614, 630 (2018) (advocating for a strict liability breach of confidence tort to apply in data breach cases)), vacated, Muransky v. Godiva Chocolatier, Inc., 939 F.3d 1278, 1279 (11th Cir. 2019) (ordering the case to be reheard en banc). The Third Circuit, also relying on law review articles, defined the tort as: "the unconsented, unprivileged disclosure to a third party of nonpublic information that the defendant has learned within a confidential relationship." Kamal v. J. Crew Grp., Inc., 918 F.3d 102, 114 (3d Cir. 2019) (quoting Vickery, supra, at 1455). Under California law, "to establish a breach of confidence claim, the plaintiff must only allege that an idea was offered and received in confidence, and later disclosed without permission." Star Patrol Enters., Inc. v. Saban Entm't, Inc., 129 F.3d 127, at *2 (9th Cir. 1997) (unpublished) (citing Davies v. Krasna, 535 P.2d 1161, 1166 (Cal. 1975)). A special relationship is not required. Id.

Brinker argues that breach of confidence, if such a claim exists under Florida law, requires "some pre-existing confidential relationship[,]" which does not exist in a "customer-restaurant relationship . . . ." (Doc. 48 at 48). Plaintiffs argue that such a relationship is not required and that they have pled an implied contractual relationship. (Doc. 53 at 45).

Whether a special relationship is required for the tort breach of confidence is immaterial here because Brinker did not disclose Plaintiffs'

information. According to Black's Law Dictionary, "disclosure" is "[t]he act or process of making known something that was previously unknown." Disclosure, BLACK'S LAW DICTIONARY (11th ed. 2019). But Brinker did not do any act that made Plaintiffs' information known—the information was stolen by third-parties. Even assuming, arguendo, that Brinker's inadequate security facilitated the theft, such a claim would lie in negligence not breach of confidence. Simply put, Brinker made no disclosure, thus, this count is due to be dismissed.

K. Rule 9(b)

Several of Plaintiffs' claims fall under Federal Rule of Civil Procedure 9(b), which requires that "[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake." Fed. R. Civ. P. 9(b); see, e.g., Gonzalez v. State Farm Lloyds, No. 7:17-CV-00017, 2017 WL 6597181, at *2 (S.D. Tex. Aug. 17, 2017) (compiling cases and stating that "courts applying Rule 9(b) to [Texas] DTPA claims . . . appear to universally apply [R]ule 9(b) regardless of the provision."); Middleton v. Cavalry Portfolio Servs., LLC, No. 216CV01760MMDPAL, 2017 WL 969182, at *4 (D. Nev. Mar. 13, 2017) ("A fraud claim under the [Nevada CFA] must meet the heightened pleading requirement under Rule 9(b)."); Kearns v. Ford Motor Co., 567 F.3d 1120, 1125 (9th Cir. 2009) (stating that fraud prong UCL cases fall under Rule 9(b)).

Traditionally, Rule 9(b) requires the plaintiff to plead the who, what, when, where, and why of a misrepresentation. However, "[f]raud by silence . . . is, by its very nature, difficult to plead with particularity." Chrysler Credit Corp. v. Whitney Nat. Bank, 824 F. Supp. 587, 598 (E.D. La. 1993) (qutotation marks omitted) (quoting Daher v. G.D. Searle & Co., 695 F. Supp. 436, 440 (D. Minn. 1988)). Courts have crafted different tests for alleging fraud by omission.[18]

---

[18] For example, Breeden v. Richmond Cmty. Coll., 171 F.R.D. 189, 195 (M.D.N.C. 1997) states:

> In order to comply with the pleading requirements of Rule 9(b) with respect to fraud by omission, a plaintiff usually will be required to allege the following with reasonable particularity: (1) the relationship or situation giving rise to the duty to speak, (2) the event or events triggering the duty to speak, and/or the general time period over which the relationship arose and the fraudulent conduct occurred, (3) the general content of the information that was withheld and the reason for its materiality, (4) the identity of those under a duty who failed to make such disclosures, (5) what those defendant(s) gained by withholding information, (6) why plaintiff's reliance on the omission was both reasonable and detrimental, and (7) the damages proximately flowing from such reliance.

Id. The Whitney National Bank court relied on only four items:

> [A] plaintiff alleging fraud by silence should be able to allege the following with reasonable particularity: (1) the information that was withheld, (2) the general time period during which the fraudulent conduct occurred, (3) the relationship giving rise to the duty to speak, and (4) what the person or entity engaged in the fraudulent conduct gained by withholding the information.

Whitney Nat. Bank, 824 F. Supp. at 598.

Despite the difficulty in pleading with particularity something that did not occur, the Eleventh Circuit's treatment of Rule 9(b) does not change for cases alleging fraudulent omission. In re Galectin Therapeutics, Inc. Sec. Litig., 843 F.3d 1257, 1269 (11th Cir. 2016). Plaintiffs must allege:

> (1) precisely what statements or omissions were made in which documents or oral representations; (2) the time and place of each such statement and the person responsible for making (or, in the case of omissions, not making) them; (3) the content of such statements and the manner in which they misled the plaintiff, and; (4) what the defendant obtained as a consequence of the fraud.

In re Galectin, 843 F.3d at 1269. Thus, Plaintiffs must allege what omissions were made in which documents or oral representations, when they should have occurred and who failed to disclose information, how the nondisclosure misled Plaintiffs, and what Brinker obtained as a result. Id.

As explained in other sections of this Order, Plaintiffs have failed to allege with particularity the fraudulent omissions they relied upon for Brinker's benefit. Although Plaintiffs have alleged that they would not have dined at Chili's had they known their personal information would not be safeguarded, they have not alleged who should have told them their information would not be secure and when and where this statement should have been made. Thus, in amending their complaint, Plaintiffs shall comply with Rule 9(b) for all claims sounding in fraud.

IV. CONCLUSION

Accordingly, it is hereby

ORDERED:

1. Due to the voluntary dismissal of Plaintiff Fred Sanders, Counts VIII and IX, brought under Virginia law, are **DISMISSED**.

2. Defendant Brinker International, Inc.'s Motion to Dismiss (Doc. 48) is **DENIED in part and GRANTED in part**:

   a. Defendant's Rule 12(b)(6) Motion to Dismiss is **GRANTED** as to Counts III, IV, V, VI, VII, XII (California UCL fraudulent business practice), and XIII. These Counts are **DISMISSED**.

   b. The Motion to Dismiss is **GRANTED in part** as to Counts X and XII (Nevada CFA). The portion of Count X alleging violations of California Civil Code § 1798.82 is **DISMISSED** but the remainder of the Count remains. The portion of Count XII(b) alleging violations of Nevada Revised Statute § 598.0917(7) is **DISMISSED** but the remainder of that Count remains.

   c. The Motion to Dismiss is **DENIED** as to Counts I, II, and XI.

3. The Court will permit Plaintiffs to replead any of the dismissed claims. However, in deciding whether to amend as to any dismissed claim, Plaintiffs should carefully consider whether amendment is appropriate or whether proceeding on the other counts which the Court has upheld is sufficient.

4. Not later than **February 28, 2020**, Plaintiffs shall file their Third Amended Consolidated Class Action Complaint.

5. Not later than **March 27, 2020**, Defendants shall file their answer or other response to the Third Amended Consolidated Class Action Complaint.

6. Not later than **March 27, 2020**, the Parties shall file a Second Revised Case Management Report detailing how the Court should proceed.

7. All new discovery in this case remains **STAYED** until the Court issues a Case Management and Scheduling Order.

DONE AND ORDERED in Jacksonville, Florida this 27th day of January, 2020.

TIMOTHY J. CORRIGAN
United States District Judge

jb
Copies:

Counsel of record